SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

[METHOD FOR HANDLING CIPHERING STATUS IN A WIRELESS NETWORK]

Background of Invention

[0001] 1. Field of the Invention

[0002] The present invention relates to a wireless communications system. More specifically, the present invention discloses a method correcting ciphering status maintenance in a wireless communications system.

[0003] 2. Description of the Prior Art

[0004] Please refer to Fig.1. Fig.1 is a simple block diagram of a prior art wireless communications system 10, as defined by the 3rd Generation Partnership Project (3GPP) specifications 3GPP TS 25.322 V3.10.0 "RLC Protocol Specification", and 3GPP TS 25.331 V3.10.0 "Radio Resource Control (RRC) Specification", which are included herein by reference. The wireless communications system 10 comprises a plurality of radio network subsystems (RNSs) 20 in communications with a core network (CN) 30. The plurality of RNSs 20 is termed a Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access Network, or UTRAN 20u for short. Each RNS 20 comprises one radio network controller (RNC) 22 that is in communications with a plurality of Node Bs 24. Each Node B 24 is a transceiver, which is adapted to send and receive wireless signals, and which defines a cell region. A plurality of Node Bs 24 defines a UTRAN Registration Area (URA). The wireless communications system 10 assigns a mobile unit 40 (generally termed a "UE" for User Equipment) to a particular RNS 20, which is then termed the serving RNS (SRNS) 20s of the UE 40.

[0005] Please refer to Fig.2. Fig.2 is a simplified block diagram of the UTRAN 20u in

wireless communications with the UE 40 of Fig.1. The UTRAN 20u communicates with the UE 40 over a plurality of radio bearers 12. The UE 40 thus has corresponding radio bearers 22, one for each of the radio bearers 12. Each radio bearer 12 has a receiving buffer 12r for holding protocol data units (PDUs) 11r received from the corresponding radio bearer 22 of the UE 40.

[0006] Each radio bearer 12 also has a transmitting buffer 12t for holding PDUs 11t that are awaiting transmission to the corresponding radio bearer 22 of the UE 40. A PDU 11t is transmitted by the UTRAN 20u along a radio bearer 12 and received by the UE 40 to generate a corresponding PDU 21r in a receiving buffer 22r of the corresponding radio bearer 22. Similarly, a PDU 21t is transmitted by the UE 40 along a radio bearer 22 and received by the UTRAN 20u to generate a corresponding PDU 11r in the receiving buffer 12r of the corresponding radio bearer 12.

[0007] For the sake of consistency, the data structures of pair entity PDUs 11t, 21r, and 21t, 11r along corresponding radio bearers 12 and 22 are identical. That is, a transmitted PDU 11t generates an identical corresponding received PDU 21r, and a transmitted PDU 21t generates an identical corresponding PDU 11r. Although the data structure of each pair entity PDU 11t, 21r, and 21t, 11r along corresponding radio bearers 12 and 22 is identical, different radio bearers 12, 22 may use different PDU data structures according to the type of connection agreed upon along the peer entity radio bearers 12, 22.

[0008] There are two distinct connection methods, or domains, within the core network 30 for carrying PDUs 11t, 21t: a circuit switched (CS) domain 30c and a packet switched (PS) domain 30p. A CS connection 30c provides a dedicated path to a single connection and no other stations can use that dedicated path until the call is finished. Circuit switching uses a constant bit rate (CBR) and is frequently called synchronous switching because the PDUs 11t, 21t are transmitted only in the specific dedicated path.

[0009] On the other hand, packet switching (PS) 30p breaks down data streams into variably sized packets (PDUs 11t, 21t) that are transmitted with a variable bit rate (VBR) in bursts over radio bearers 12, 22 that are shared with other stations on a first come, first serve basis. For this reason, packet switching is often referred to an

asynchronous switching.

[0010] In general, every PDU 11r, 11t, 21r and 21t will have a sequence number 5r, 5t, 6r, 6t. The sequence number 5r, 5t, 6r, 6t is an m-bit number that is incremented for each PDU 11r, 11t, 21r, 21t. The magnitude of the sequence number 5r, 5t, 6r, 6t indicates the sequential ordering of the PDU 11r, 11t, 21r, 21t in its buffer 12r, 12t, 22r, 22t. For example, a received PDU 11r with a sequence number 5r of 108 is sequentially before a received PDU 11r with a sequence number 5r of 109, and sequentially after a PDU 11r with a sequence number 5r of 107. The sequence number 5t, 6t is often explicitly carried by the PDU 11t, 21t, but may also be implicitly assigned by the UTRAN 20u or UE 40. For example, in an acknowledged mode (AM) setup for corresponding radio bearers 12 and 22, each transmitted PDU 11t explicitly carries a 12-bit sequence number 5t; successful reception of each transmitted PDU 11t generates an identical corresponding PDU 21r and is acknowledged as received by the UE 40 by using the sequence number 6r of the received PDU 21r.

[0011] A 12-bit sequence number 5t is explicitly carried by each PDU 11t in acknowledged mode transmissions. The UE 40 scans the sequence numbers 6r embedded within the received PDUs 21r to determine the sequential ordering of the PDUs 21r, and to determine if any PDUs 21r are missing. The UE 40 can then send a message to the UTRAN 20u that indicates which PDUs 21r were received by using the sequence numbers 6r of each received PDU 21r, or may request that a PDU 11t be re-transmitted by specifying the sequence number 5t of the PDU 11t to be re-transmitted.

[0012] Alternatively, in an unacknowledged transmission mode (UM), 7-bit sequence numbers 5t, 6t are explicitly carried by the transmitted PDUs 11t, 21t, but received PDUs 11r, 21r are not acknowledged as successfully received. In certain special cases, such as a transparent transmission mode, sequence numbers are not even assigned to PDUs 11t, 11r, 21t, 21r.

[0013] The PDUs 11t and 21t are generally not transmitted "out in the open". A ciphering engine 14 on the UTRAN 20u and a corresponding ciphering engine 24 on the UE 40 together ensure secure and private exchanges of data exclusively between the UTRAN 20u and the UE 40. A function of the ciphering engine 14, 24 is the obfuscation (i.e.,

ciphering, or encryption) of data held within a transmitted PDU 11t, 21t so that the corresponding PDU 11r, 21r presents a meaningless collection of random numbers to an eavesdropper.

[0014] PS domain 30p and CS domain 30c connections can simultaneously co-exist between the UTRAN 20u and the UE 40 and one, none, or both of the PS and the CS domains 30p, 30c can make use of ciphering. Therefore, when transmitting a PDU 11t, the ciphering engine 14 uses, amongst other inputs, a ciphering key 14p (for PS domain 30p connections) and a ciphering key 14c (for CS domain 30c connections) to perform ciphering functions upon a PDU 11t.

[0015] To properly decipher a corresponding PDU 21r, the corresponding ciphering engine 24 must use an identical ciphering key 24p or 24c depending on the specific domain 30p, 30c currently in use. The ciphering keys 14p, 24p, and 14c, 24c are different for the respective domains but remain constant across all PDUs 11t, 21t within a specific domain (and thus corresponding PDUs 21r, 11r) and radio bearers 12, 22, until explicitly changed by both the UTRAN 20u and the UE 40.

[0016] Changing of the ciphering keys 14p, 24p and 14c, 24c is effected by a security mode reconfiguration process that involves handshaking between the UTRAN 20u and the UE 40 to ensure proper synchronization of the ciphering engines 14, 24. The UTRAN 20u typically initiates the security mode reconfiguration process. Security mode reconfiguration is used to change the ciphering keys 14p, 24p and 14c, 24c and to both activate and deactivate ciphering of transmitted PDUs 11t, 21t.

[0017] Security mode reconfiguration is a somewhat complicated process that involves several steps. One of the initial steps is the transmitting by the UTRAN 20u of a ciphering reconfiguration message, a so-called security mode command, along a special signaling radio bearer 12s to the UE 40. The security mode command indicates the new ciphering configuration that is to be used by the UTRAN 20u and the UE 40, such as the use of the new ciphering key 14n, 24n, or the activation or deactivation of PDU 11t, 21t ciphering.

[0018] Note that the security mode command is itself carried by one or more PDUs 11t, and thus may be enciphered under the old ciphering configuration, i.e., using the

ciphering key 14p or 14c depending on the domain for which the most recent security negotiation took place. The radio bearer 12s is an acknowledged mode radio bearer, and thus the UE 40 will explicitly acknowledge using the radio bearer 22s the successful reception of each PDU 11t that carries the security mode command as shown in Fig.3. In this manner, the UTRAN 20u can be certain that the security mode command was received and processed by the UE 40.

[0019] An Information Element (IE) has an enumerated variable maintaining a ciphering status 25 in the UE 40 holding information about the current status of ciphering in the UE 40, and can be set to either "Not started" or "Started". The UTRAN 20u comprises a corresponding variable 15 to maintain the ciphering status information in the UTRAN 20u. When a security mode command is received by the UE 40 indicating the activation of PDU 11t, 21t ciphering, the ciphering status variable 25 in the UE 40 is set to "Started". When a security mode command is received by the UE 40 indicating the deactivation of PDU 11t, 21t ciphering, the ciphering status variable 25 in the UE 40 is set to "Not started". When transmitting PDUs 21t or receiving PDUs 21r, the UE 40 checks the value of the variable ciphering status 25 to determine if ciphering is to be used to encrypt/decrypt the PDUs 21t, 21r. If the value of the ciphering status variable 25 is set to "Not started", ciphering is not used. If the value of the ciphering status variable 25 is set to "Started", the ciphering engine 24 and the ciphering key 24c or 24p is be used, depending upon the domain 30p, 30c of the associated radio bearer 22.

[0020] A problem in the prior art occurs when the UTRAN 20u and the UE 40 are using both the PS domain and the CS domain for wireless communications. Although the ciphering keys 14p, 24p and 14c, 24c are domain specific, the ciphering status variable 25 is not domain specific because there is only one ciphering status variable 25 in the UE 40.

[0021] For example, consider the following scenario:

[0022] 1) A PS connection is established and a security mode command is sent from the UTRAN 20u to the UE 40 initiating a security mode control procedure to start ciphering for the PS domain. The ciphering status variable 25 is set to "Started" and ciphering is started for the PS connection.

[0023] 2) A CS connection is subsequently established between the UTRAN 20u and the UE 40, and the UTRAN 20u does not send a security mode command to the UE 40 specifying that ciphering is to be used in the CS connection. Therefore, the UTRAN 20u is sending and expects to receive un-ciphered PDUs 11r, 11t when using the CS mode connection. However, when the UE 40 transmits or receives the respective PDUs 21t or 21r, the UE 40 checks the value of the ciphering status variable 25 to determine if ciphering is to be used with the PDUs 21t, 21r. Consequently, the UE 40 begins ciphering of the CS PDUs 21t, 21r because the ciphering status variable 25 was previously set to a value of "Started" by the security mode command intended only for the PS connection. Obviously, using the ciphering engine 14 in this situation has undesirable consequences and results in the PDUs 21t, 21r being converted into a meaningless collection of random numbers.

Summary of Invention

[0024] It is therefore an objective of the claimed invention to correct the handling of ciphering status in a wireless communications system to prevent inadvertent ciphering when establishing a new domain connection.

[0025] Briefly summarized, the preferred embodiment of the claimed invention includes a wireless communications system having a Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access Network (UTRAN), commonly referred to as a base station, in wireless communications with a mobile unit, commonly referred to as user equipment (UE).

[0026] The UTRAN can transmit protocol data units (PDUs) to the mobile unit and receive PDUs from the UE using a packet switched (PS) domain connection or a circuit switched (CS) domain connection. Both the PS and CS domain PDUs can be transmitted in a ciphered or an un-ciphered configuration, respectively. The UE includes a first ciphering status variable indicating the ciphering status, meaning the activation or deactivation of ciphering, of the PS domain PDUs, and a second ciphering status variable indicating the ciphering status of the CS domain PDUs.

[0027]

When the UTRAN transmits a security mode command indicating that ciphering is to be activated or deactivated for the PDUs in the PS domain, the first ciphering status

variable is set according to the security mode command. When the UTRAN transmits a security mode command indicating that ciphering is to be activated or deactivated for the PDUs in the CS domain, the second ciphering status variable is set according to the security mode command.

[0028] When the UE receives a PS domain PDU from the UTRAN, the UE determines whether the received PDU is to be decoded based on the value of the first ciphering status variable. When the UE transmits a PS domain PDU to the UTRAN, the UE determines whether the PDU awaiting transmission is to be encoded before transmission based on the value of the first ciphering status variable.

[0029] When the UE receives a CS domain PDU from the UTRAN, the UE determines whether the received PDU is to be decoded based on the value of the second ciphering status variable. When the UE transmits a CS domain PDU to the UTRAN, the UE determines whether the PDU awaiting transmission is to be encoded before transmission based on the value of the second ciphering status variable.

[0030] A second embodiment of the claimed invention is similar to the first embodiment with the addition of setting the first ciphering status variable to indicate the deactivation of ciphering when a PS connection is first being established and setting the second ciphering status variable to indicate the deactivation of ciphering when a CS connection is first being established. Deactivating ciphering for a given domain when that given domain is being established ensures that ciphering will not be performed on the PDUs within that domain unless a security mode command specifically activating ciphering within that domain is received by the UE from the UTRAN.

[0031] It is an advantage of the claimed invention to maintain one ciphering status variable for the PS domain and a separate ciphering status variable for the CS domain so that inadvertent ciphering of PDUs is avoided.

[0032] These and other objectives of the claimed invention will no doubt become obvious to those of ordinary skill in the art after reading the following detailed description of the preferred embodiment, which is illustrated in the various figures and drawings.

Brief Description of Drawings

[0033] Fig.1 is a simplified block diagram of a prior art wireless communications system.

[0034] Fig.2 is another simplified block diagram of the wireless communications system of Fig.1.

[0035] Fig.3 is a message sequence chart for a security mode command in the wireless communications system of Fig.1.

[0036] Fig.4 is a simplified block diagram of a wireless communications system according to the present invention.

[0037] Fig.5 is a simplified block diagram of a mobile unit in a wireless communications system according to the present invention.

Detailed Description

[0038] Fig.4 is a simplified block diagram of a wireless communications system according to the present invention. The embodiment of a wireless communications system has a Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access Network (UTRAN) 60u, commonly referred to as a base station 60u, in wireless communications with a mobile unit 80, commonly referred to as user equipment (UE) 80. The UTRAN 60u provides the UE 80 with access to a core network 90.

[0039] The UTRAN 60u communicates with the UE 80 using a plurality of radio bearers 52, and the UE 80 communicates with the UTRAN 60u using a plurality of radio bearers 62, each radio bearer 52 corresponding to a radio bearer 62. Each radio bearer 52,62 has a receiving buffer 52r, 62r for receiving the protocol data units (PDU) 51r, 61r, and a transmitting buffer 52t, 62t for holding the PDUs 51t, 61t awaiting transmission.

[0040] Communications between the UTRAN 60u and the UE 80 use a packet switched (PS) domain 90p transmission mode and/or a circuit switched (CS) domain 90c transmission mode. Additionally, the UTRAN 60u and the UE 80 have ciphering engines 54 and 64 respectively to encrypt or decrypt the PDUs 51r, 51t, 61r, 61t using a key 54c, 64c for CS PDUs 51r, 51t, 61r, 61t, and a key 54p, 64p for PS PDUs 51r, 51t, 61r, 61t. The ciphering of the PS and CS PDUs 51r, 51t, 61r, 61t is optional and is domain dependent so that all the PDUs 51r, 51t, 61r, 61t within a given domain are

ciphered or all the PDUs 51r, 51t, 61r, 61t within a given domain are not ciphered. That is, peer entity radio bearers 52, 62 are both associated with one of the domains 90c, 90p within the core network 90, i.e., with the CS domain 90c or the CS domain 90c, and perform ciphering accordingly.

[0041] The UE 80 includes a first ciphering status variable 65p indicating the ciphering status of the PS domain 90p PDUs 61r, 61t, and a second ciphering status variable 65c indicating the ciphering status of the CS domain 90c PDUs 61r, 61t. The ciphering status variable 65p indicates whether ciphering is activated or deactivated for the PS domain 90p, and the ciphering status variable 65c indicates whether ciphering is activated or deactivated for the CS domain 90c.

[0042] When the UE 80 receives a security mode command from the UTRAN 60u indicating that ciphering is to be activated or deactivated for the PDUs 61r, 61t in the PS domain 90p, the first ciphering status variable 65p is set to a value of "Not started" or "Started", according to the PS domain security mode command. When the UE 80 receives a security mode command from the UTRAN 60u indicating that ciphering is to be activated or deactivated for the PDUs 61r, 61t in the CS domain 90c, the second ciphering status variable 65c is set according to the CS domain security mode command.

[0043] When the UE 80 receives a PS domain PDU 61r from the UTRAN 60u, the UE 80 determines whether the received PDU 61r is to be decrypted based on the value of the first ciphering status variable 65p. When the UE 80 transmits a PS domain PDU 61t to the UTRAN 60u, the UE 80 determines whether the PDU 61t awaiting transmission is to be encrypted before transmission based on the value of the first ciphering status variable 65p.

[0044] Similarly, when the UE 80 receives a CS domain PDU 61r from the UTRAN 60u, the UE 80 determines whether the received PDU 61r is to be decrypted based on the value of the second ciphering status variable 65c. When the UE 80 transmits a CS domain PDU 61t to the UTRAN 60u, the UE 80 determines whether the PDU 61t awaiting transmission is to be encrypted before transmission based on the value of the second ciphering status variable 65c.

[0045] A second embodiment of the claimed invention is similar to the first embodiment with the addition of the UE 80 ensuring that ciphering is deactivated for a given domain 90c, 90p before establishing an initial connection using that domain 90c, 90p. The UE 80 sets the first ciphering status variable 65p to indicate the deactivation of ciphering when a PS connection is being established and no other PS connections exist. It is possible to have two or more same-domain 90c, 90p simultaneous connections and the UE 80 has already received a security mode command activating ciphering for that domain 90c, 90p. Therefore, the second embodiment UE 80 deactivates ciphering for the PS domain 90p when a PS domain connection is being established only if no other PS connections exist at the time. Similarly, the UE 80 deactivates ciphering via the second ciphering status variable 65c when a CS connection is being established and no other CS connections exist. Deactivating ciphering for a given domain 90c, 90p when that given domain 90p, 90c is newly established ensures that ciphering will not be performed on the PDUs 61r, 61t within that domain 90p, 90c unless a security mode command specifically activating ciphering transmissions for that domain 90p, 90c is received by the UE 80 from the UTRAN 60u.

[0046] With regard to the above embodiments for the UE 80, it should be understood that corresponding embodiments must be implemented for the UTRAN 60u to ensure proper ciphering synchronization between the UE 80 and the UTRAN 60u. That is, the UTRAN 60u should also maintain ciphering status variables (55c, 55p of Fig.4) that are synchronized with those of the UE 80 (65c, 65p). Such synchronization is assured by simply having the UTRAN 60u follow the method disclosed for the UE 80, and should be clear to one reasonably skilled in the art.

[0047] Fig.5 is a simplified block diagram of an example UE 100 according to the present invention. The UE 100 comprises a keypad 102 for data entry, an LCD 104 for displaying data, a transceiver 108 for communicating with a wireless communications system, and control circuitry 106. The control circuitry 106 comprises a CPU 106c to process controlling instructions and a memory 106m for storing data and protocol information. The memory 106m comprises a program code segment 107 and a location for storing a first ciphering status variable 110C and a second ciphering status variable 110p. The functions of the first ciphering status variable 110C and a

second ciphering status variable 110p in the UE 100 are the same as the functions of first ciphering status variable 65p and the second ciphering status variable 65c in the UE 80.

[0048] In contrast to the prior art, the present invention maintains one ciphering status variable 65p for the PS domain 90p, and a separate ciphering status variable 65c for the CS domain 90c. The maintenance of separate and domain specific ciphering status variables 65p, 65c allows independent control of ciphering for each domain 90p, 90c. Independent control precludes inadvertent ciphering of the PDUs 51r, 51t, 61r, 61t within a newly established wireless communication connection.

[0049] Those skilled in the art will readily observe that numerous modifications and alterations of the method may be made while retaining the teachings of the invention. Accordingly, the above disclosure should be construed as limited only by the metes and bounds of the appended claims.